

## REMARKS

In the first office action that was mailed on 04/02/2004 claims 1, 2, 4-13 and 20-46 were rejected under 35 U.S.C. 102(b) as being anticipated by Chi (U.S. 5,978,917), claim 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Chi, and further in view of Chambers (U.S. 5,398,196), and claims 14-19 were rejected under 35 U.S.C. 103(a) as being unpatentable over Chi. A response was filed on 04/16/2004, wherein none of the claims were amended.

In the second office action that was mailed on 08/09/2004 the Examiner rejected claims 1, 2 and 4-46 under 35 U.S.C. 103(a) as being unpatentable over Chi and further in view of a newly cited U.S. Patent to McLain, Jr. (U.S. 5,812,826). Claim 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Chi and McLain, and further in view Chambers (U.S. 5,398,196). A response was filed on 11/02/2004, wherein none of the claims were amended.

In the third office action the Examiner has now rejected claim 1 under 35 U.S.C. 112, second paragraph for the reasons of record, and has rejected claims 1-46 under 35 U.S.C. 103(a) as being unpatentable over the newly cited Schnurer et al. (U.S. 5,842,002) in view of Nachenberg (U.S. 5,826,013), previously cited by the applicants in the Information Disclosure Statement filed with the application. These rejections are also respectfully disagreed with, and are traversed below.

With regard to the rejection of claim 1 under 35 U.S.C. 112, second paragraph, claim 1 does not state that the isolated network is connected to another network. Claims 1 recites in part "an isolated network that does not have a direct connection to another network that is not an isolated network". Clearly, if the isolated network did have a connection to another network that was also an isolated network, then the isolated network would still be isolated. Note that the specification states at page 4, lines 14-18, that:

"In a preferred embodiment, the software being analyzed is effectively confined to the analysis network environment, and cannot in fact read information from, or alter any information on, any production network or the global Internet."

Reference can also be had to Fig. 2 and to the specification at, for example, page 8, lines 22-32.

It is respectfully submitted that one skilled in the art when reading claim 1, in view of the specification and claims, would not find the language of claim 1 to be vague or indefinite.

The Examiner is respectfully requested to reconsider and remove the rejection of claim 1 under 35 U.S.C. 112, second paragraph.

Turning now to the rejection of claims 1-46 under 35 U.S.C. 103(a) in view of Schnurer et al. and Nachenberg, the applicants have reviewed the cited U.S. Patents, and note that Nachenberg does not teach an isolated network. The applicants further note that while Schnurer et al. may mention 'emulation', what this U.S. Patent actually teaches is trapping data coming in from a network (which apparently also includes removable media), placing it in an emulation environment (emulation box), and attempting to determine whether it contains a virus. However, the applicants note that Schnurer et al. are silent as to what occurs if the data being analyzed in the emulation environment is a program that attempts to communicate with other programs over the network. This is a problem that the applicants have recognized and addressed in the instant patent application.

What Nachenberg actually teaches is a very specific technique within the emulation space for using specific knowledge (presumably gathered by humans rather than determined automatically, although Nachenberg is not specific) about certain encryption engines to control the execution of the emulator.

More specifically, the Examiner states that Nachenberg teaches that the execution component is coupled to an isolated network that does not have a direct connection to another network that is not an isolated network (see column 5, lines 62-67, column 4, lines 1-40). The Examiner's characterization of the reference is not understood, as there is not seen to be any mention of a network, isolated or otherwise, in this section of Nachenberg. What is stated at, for example, col. 5, lines 62-67, is simply:

"Referring now to FIG. 1C, there is shown an executable image 100" infected by a polymorphic virus 150. Polymorphic virus 150 comprises a static virus body 160 including a mutation engine 162, both of which are shown hatched in the FIG. 1C to indicate their encrypted state. On infection, mutation engine 162 generates a variable encryption routine (not shown) that encrypts static virus body 160 (including mutation engine 162) to prevent detection of polymorphic virus 150 by conventional scanning techniques."

In fact, a word search of Nachenberg finds occurrences of the word "network" only in the list of references cited, and the word "isolated" does not appear at all.

This being the case, the Examiner's use of Nachenberg for purportedly teaching an execution component coupled to an isolated network is respectfully disagreed with. Further, since the Examiner specifically admits that Schnurer et al. do **not** teach an "execution component being coupled to an isolated network...", then the proposed combination of Schnurer et al. and Nachenberg does not teach or suggest this subject matter.

The Examiner also states that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Schnurer et al.'s system for trapping computer viruses with Nachenberg's method for emulating a polymorphic virus detection module which would allow monitoring and disruptive network behavior prior to emulating the target program, and refers to Nachenberg at column 3, lines 37-46).

Nachenberg at column 3, lines 37-46, states simply that:

"The dynamic exclusion module (240) examines the instruction/interrupt usage profiles (224) of each known polymorphic virus (150) as each instruction is fetched for emulation. The instruction/interrupt usage profiles (224) indicate which polymorphic viruses (150) employ mutation engines that do not use the fetched instruction in decryption loops they generate, and the emulation control module (220) flags these viruses. The emulation control module (220) continues until all mutation engines have been flagged or until a threshold number of instructions have been emulated."

The Examiner's characterization is not understood. "Monitoring [for?] disruptive network

behavior prior to emulating the target program" is not seen to be technically appropriate, since before running the target there would presumably not be any disruptive network behavior (without admitting that Nachenberg discusses a network).

Based at least on the foregoing argument, it can be seen that the proposed combination of references, without admitting that the proposed combination is suggested or technically feasible, would not suggest the subject matter of claim 1 to one skilled in the art. In that claim 1 is clearly patentable, then dependent claims 2-26 are also clearly patentable.

Further in this regard, and using claim 2 as an example, the Examiner states that Schnurer et al. teaches the emulation component further comprises a server programmed so as to return emulated results in response to a request resulting from the software program being executed on the execution component, and refers to column 7, lines 19-52. It is respectfully submitted that Schnurer et al. does not teach this subject matter at column 7, lines 19-52. What is stated there is instead:

"Upon startup of the trapping device 10, the emulation software is read from EPROM 14 and executed. When a user turns on his workstation 38, a connection is established between the workstation 38 and the file server 30 (or 42). A connection session is created in the RAM 16 of the CPU 12. In like fashion, a session is created for each user.

As the user at a workstation 38 runs commands and moves file about, data is ultimately written to and read from the file server 30. The trapping device 10 splits the data into two paths. One path connects directly to the protected computer system 28 without modification. Data over the other path is written into the emulation box or virtual world created for each user. The write is performed in this box just as it would have been performed on the file server 30, protected computer 28 or workstation 38. Changes in data and time are simulated to trigger time sensitive viruses, fooling then as to the actual data and time. If the environment changes, it is checked to determine whether simply data was written or whether executable code was written.

Once the executable in inside the emulation box, a Cyclic Redundancy Check (CRC) is made of the Interrupt Request table (IRQ). Also, CRCs are generated on all files that are placed in the emulation box. The CRC is an error detection and correction code widely used in the computer and engineering fields. Other

aspects of the environment, such as available memory, are saved too. All information saved is stored outside of the emulation box where it cannot be altered by a virus. The executable is forced to run.

If absolutely nothing happens, a self replicating virus does not exist. If anything within the environment changes (i.e. size of files, sudden attempts to write to other executables in the emulation box, etc.) it is determined that a virus does exist and is attempting to self replicate itself."

This portion of Schnurer et al. clearly does not disclose the subject matter of claim 2.

Further, and with regard to claims 14, 15, 16, 17, 18 and 19, the applicants do not expressly or impliedly admit that they are in agreement with the Examiner's taking of Official Notice for the claimed subject matter.

Independent claim 27 recites in part:

"an emulated data communications network having at least one emulated network server coupled thereto, said at least one emulated network server responding to requests received from said emulated data communications network;

an emulated host computer coupled to said emulated data communications network, said emulated host computer for executing the software program, the software program operating to originate requests to said emulated data communications network;

at least one emulated goat computer coupled to said emulated data communications network; and

at least one monitor for detecting an occurrence of the desired behavior in at least one of said emulated network server, said emulated host computer, and said at least one emulated goat computer."

The Examiner has rejected this claim, and dependent claims 28-36, "because of similar rationale outlined above" (i.e., in the rejection of claims 1-26). Since it has been clearly shown that the Examiner's rationale for rejecting claims 1-26 as being unpatentable over Schnurer et al. in view of Nachenberg is not supported by the actual teachings of these U.S. Patents, then the use of these U.S. Patents to reject claims 27-36 is also not appropriate. Claims 27-36 are clearly allowable

over the proposed combination of Schnurer et al. in view of Nachenberg.

Independent claim 38 is drawn to a computer program causing execution of a method for:

"emulating a data communications network having at least one emulated network server coupled thereto, said at least one emulated network server operating to respond to requests received from said emulated data communications network;

emulating a host computer coupled to said emulated data communications network, said emulated host computer executing the software program, the software program operating to originate requests to said emulated data communications network; and

detecting an occurrence of the behavior in at least one of said emulated network server and said emulated host computer."

The Examiner has rejected this claim, and dependent claims 38-46, "because of similar rationale outlined above" (i.e., in the rejection of claims 1-26). Since it has been clearly shown that the Examiner's rationale for rejecting claims 1-26 as being unpatentable over Schnurer et al. in view of Nachenberg is not supported by the actual teachings of these U.S. Patents, then the use of these U.S. Patents to reject claims 37-46 is also not appropriate. Claims 37-46 are clearly allowable over the proposed combination of Schnurer et al. in view of Nachenberg.

The Examiner is respectfully requested to reconsider and remove the expressed rejections, and to allow claims 1-46 as originally filed. However, should there be any remaining issue that would impede the allowance of all of the pending claims, then the Examiner is respectfully requested to contact the undersigned attorney through any of the means set forth below.

S.N. 09/640,453  
Art Unit: 2137



Respectfully submitted:

A handwritten signature in black ink that reads "Harry Smith".

Harry F. Smith

A handwritten date in black ink that reads "5/31/2005".

Date

Reg. No.: 32,493

Customer No.: 29683

HARRINGTON & SMITH, LLP

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400

Facsimile: (203)944-0245

email: hsmith@hspatent.com

#### **CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

May 31, 2005  
Date

Elba Poggetti  
Name of Person Making Deposit